914-TDA-259

EOSDIS Maintenance and Development Project

F-Secure Secure Shell 3.3.0 Maintenance Upgrade for the EOSDIS Core System (ECS) Project

Release Notes

May 2004

Raytheon Company
Upper Marlboro, Maryland

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this release is to implement a newer, more capable version of F-Secure Secure Shell (ssh) COTS package and to improve the overall performance of the product over Wide Area Networks (WANs).

1.2 Scope

This document describes the contents of the package F-Secure Secure Shell 3.3.0. The document identifies the baseline and patch level of the delivery. It also provides an inventory of the delivery, a list of fixed NCRs, and special operating instructions where applicable.

The CCR number that releases this document is 04-XXXX "Baseline F-Secure Secure Shell 3.3.0 Server".

1.3 Impact

This version implements a number of fixes to ssh that will improve operational robustness and is faster. DAACs are also encouraged to install the new version due to a possible vulnerability in ASN.1 encoding in the existing version. Not implementing this upgrade will mostly result in lower throughput of ssh applications.

This page intentionally left blank.

2 Related Documentation

2.1 ECS Baseline Documents

910-TDA-003	COTS SW Version B/L Report
910-TDA-023	Critical COTS Software List
920-TDE-002	LP DAAC Hardware Software Map
920-TDL-002	LaRC DAAC Hardware Software Map
920-TDN-002	NSIDC DAAC Hardware Software Map
920-TDG-002	GES DAAC Hardware Software Map
920-TDV-002	VATC Hardware Software Map
920-TDP-002	PVC Hardware Software Map
920-TDS-002	SMC Hardware Software Map

2.2 Vendor Documents

Ssh330unix.pdf	F-Secure SSH for UNIX documentation (in tar file)

This page intentionally left blank.

3 General Package Description

3.1 General Product

Secure Shell is a secure replacement of the Berkeley "R" commands such as rlogin, rsh, rcp and rexec. This release implements a newer version of the second-generation version of secure shell called ssh protocol 2. Packages are included for Sun Solaris 8, SGI IRIX 6.5.X and Red Hat Linux. The product is modified from the original source code to improve Wide Area Network (WAN) throughput by increasing the default window sizes available to applications. The packages for TCP Wrappers version 7.6 are also included in order to have all the pieces together in package but there is no change from when the last update occurred in ECS SSH version 2.1.

3.2 New/Added Capabilities or Major Fixes

3.2.1 F-Secure Changes

From F-Secure documentation, these are the changes since ssh 3.2.3

F-Secure SSH for UNIX 3.3.0 build 14

- README and other documentation files updated.
- build system: New versions of config.guess, config.sub and missing, updated the rpm spec file to allow extra option passing.

F-Secure SSH for UNIX 3.3.0 build 13

- Fixed certificate authentication compatibility code with older clients sending signature over MD5 hash.

F-Secure SSH for UNIX 3.3.0 build 12

- sshd2: New config option, DontFork - controls whether or not the server should fork after starting. Default is no (to fork).
- New config option, SessionRestricted - controls what kind of sessions can be requested from the server. Comma-separated list containing one or more of shell, exec and subsystem.
- Backed out some pointless calls to ssh_ofree() in session code.

F-Secure SSH for UNIX 3.3.0 build 11

- rpm spec file: Place the sshd2 init script in a default location.
- ssh-sysinfo: Removed this tool, it ended up not being useful.

F-Secure SSH for UNIX 3.3.0 build 10

- ssh client: New configuration option, ConnectionTimeout, decides how long the client shall wait until returning from a connection attempt.
- local password authentication: PermitEmptyPassword works now on all systems, previously only worked on AIX.
- sshreadline: Fixed a small oversight that broke comment editing in ssh-keygen2.
- server configuration: Use internal sftp server by default.

F-Secure SSH for UNIX 3.3.0 build 9

- sshnet: Try gethostbyname() if getipnodebyname() fails. This can happen when not using DNS for name resolving. Note that in this case DNS overrides any local name resolving as getipnodebyname() is tried before gethostbyname().
- sftp: Display help for chmod and lchmod.
- ssh2: Show help for -i option.
- sshregexp: Debug level raised from 8 to 12.

F-Secure SSH for UNIX 3.3.0 build 8

- sshnet: Merged SSH.COM 4.0 sshnet code for most part, fixes name resolving under IA64 HP/UX with IPV6 interfaces.
- ssholdadt: Removed some dead code.
- build system: New versions of config.guess and config.sub, updated the rpm spec file.

F-Secure SSH for UNIX 3.3.0 build 7

- ssh1 compatibility: With traditional compatibility mode remove some option (-o) arguments from the list of arguments passed to ssh1.
- build system: configure argument --disable-generate-host-key disables host key generation on 'make install'. Also added an rpm spec file.
- sessions: Fixed environment variable expansion

F-Secure SSH for UNIX 3.3.0 build 6

- Allow SshBinDir setting in configuration file for binary relocation.
- build system: Some minor tweaking. Ssh header files are no longer installed with 'make install' unless --with-devel was specified on the ./configure line. Autoconf templates are now in configure.in.

F-Secure SSH for UNIX 3.3.0 build 5

- ssh-certview: Be more verbose when validating a certificate.
- scp2: Don't delete source files (if -u was specified) in the case the transfer fails.

F-Secure SSH for UNIX 3.3.0 build 4

- pubkey auth: Fix the 'ask passphrase three times for a public key' feature introduced in 3.3.0-1
- apps/ssh: New target for make, 'stripped' to strip binaries.
- Merged SSH.COM's code from versions 3.2.5 to 3.2.9.

Quoted from 'CHANGES':

- ssh2,sshd2: (by Patrick Irwin): Critical security fix: fixed several bugs in ASN.1 decoding functionality, which were caused by invalid assumptions on the format of input BER data. Certificates malformed in certain ways could cause a crash or buffer overflow. No known exploits at this time, but you are strongly advised to upgrade. Admins unwilling or unable to upgrade need to disable certificates, but this may not be enough for "hostbased" authentication. "publickey" auth should be safe even with the old version with certificates disabled. Clients are probably vulnerable against malicious servers in the initial key exchange regardless of configuration.
- ssh-keygen2: Fixed key editing.
- configure: Support (only) autoconf 2.5x.
- ssh-certview: A new option (-a) that checks that a certificate is signed by another certificate's public key.

F-Secure SSH for UNIX 3.3.0 build 2.1

- sshuserfiles: Fix some problems with the previous fix.
- sshreadline: Check for EINTR in tcsetattr/tcgetattr.
- sftp: Check local and remote connections before get or put.
- Solaris: Read the /etc/default/init file for locale and timezone environment variables.

F-Secure SSH for UNIX 3.3.0 build 1

- sshuserfiles: Handle SIGCHLD and create wrappers for calls to read and fgets to ignore EINTR.
- configure: Added --without-ncurses in case we want to make sure we won't link with libncurses.
- configure: Check that automake is 1.4 and autoconf is 2.13.
- configure: Added --without-autox that disables the usage of automake and friends, useful if incorrect version is installed.
- configure: New config.guess (2003-07-02) and config.sub.

- sftp: Added chmod command.
- filetransfer: Flush stdout after writing the progress bar.
- server: Fixed forced commands in public keys; Made it possible to add an informational message to forced commands.
- ssh-certview: Handle PEM certificates.
- client: Ignore 'Protocol' option.
- scp: Don't think that we have a remote filename if it contains slashes, also let users explicitly mark filenames as local by prepending them with a colon.
- sshd: Accept -V (show version number) without complaints.
- ssh-sysinfo: New tool for getting simple system information that might be useful for support personnel (NOTE: This is removed in the more recent versions).
- tcp forwarding: Allow forwarding from any address if the forwarding was requested for 0.0.0.0.
- public key authentication: Inquire public key passphrase three times before falling back to other authentication methods. Also remember to disable public key method when doing so.

The following capabilities have been added:

The main new features in F-Secure SSH Server and Client 3.3.0 are:

- The SFTP client now includes the chmod command

  The chmod command changes the permission of files and works in the same manner as the chmod system command found on most UNIX systems.

- New server configuration options:
  - IgnoreRlogin - The SSH server's handling of the AIX rlogin flag can now be specified in the server config file by changing the value of the IgnoreRlogin configuration option. This was previously a compile-time option.
  - DontFork - Controls whether or not the server should fork after starting.
  - SessionRestricted - Controls what kind of sessions can be requested from the server. This must be a comma-separated list containing one or more of shell, exec, subsystem.
- New client configuration option:
  - ConnectionTimeout - Specifies the maximum time in seconds that the client will wait when connecting to a server. By default, the client will wait until the operating system returns.

- Use ssh-certview to verify the signature of a certificate - The certificate helper tool ssh-certview can now also be used to verify if a user's certificate has been signed by a CA's public key.

3.2.2 EMD Changes

As secure ingest, secure distribution and Machine-to-Machine Gateway applications have grown in use, the file transfer performance was not keeping pace. One of the main reasons for upgrading now was to improve the throughput of all ssh applications but especially scp and sftp. In consultation with F-Secure, the default window sizes for each version has been changed. In the f-secure-ssh-3.3.0/apps/ssh/sshchsession.c file the following defines were changed:

Original

```
#define SSH_SESSION_INTERACTIVE_WINDOW                10000
#define SSH_SESSION_NONINTERACTIVE_WINDOW            100000
#define SSH_SESSION_INTERACTIVE_PACKET_SIZE             512
#define SSH_SESSION_NONINTERACTIVE_PACKET_SIZE         8192
```

Updated

```
#define SSH_SESSION_INTERACTIVE_WINDOW               131072
#define SSH_SESSION_NONINTERACTIVE_WINDOW            262144
#define SSH_SESSION_INTERACTIVE_PACKET_SIZE             512
#define SSH_SESSION_NONINTERACTIVE_PACKET_SIZE         8192
```

The distribution includes the software in the appropriate Operating System package. The Solaris distribution is in “pkgadd” format, the IRIX distribution is in “inst” format and the Linux distribution is in “rpm” format. Each distribution was compiled at Landover because of a bug in the X11 Security Extensions implementation, which was compiled out. Since each distribution had to be recompiled, they were recompiled with the almost identical options. The native c compiler was used for the IRIX compile but the gnu 2.9.6 compilers were used for both Solaris and Linux. The gnu compiler was used on Solaris at the recommendation of F-Secure and because of difficulties using the native Solaris 8 compiler. The configure line used for Solaris and Linux was:

% **./configure --with-libwrap --without-x11-security** ↵

For the IRIX configure, the line was:

% **./configure --with-libwrap --without-x11-security CFLAGS=’-mips3’** ↵

CFLAGS=’-mips3’ was required in order to compile for the lowest common denominator SGI architecture.

A few installation bugs have been fixed in this release:

- An upgrade from ssh 3.2.3 will not affect the system ssh2_config and sshd2_config files
- The /etc/syslog.conf file is backed up on each install

- The /etc/ssh2/ssh2_config and /etc/ssh2/sshd2_config files were changed to remove "allowedauthentication password" because the keyboard-interactive already uses password and including both allows six tries rather than three, quiet mode was set to no to make 'ssh –h' work correctly.
- The /etc/ssh2/sshd2_config file was changed to turn off printing the message of the day and will not do an email check and quiet mode was set to no to make 'ssh –h' work correctly.
- The file 'ssr.exp' was changed to update a few of the remote target hosts.

3.3 Affected Subsystem(s)

All Subsystems.

Secure shell is a part of the network infrastructure and as such indirectly participates in the operation of all ECS sub-systems. It is used directly in the Machine-to-Machine Gateway (MTMGW) and the secure file transfer applications of Ingest and Storage Management.

3.4 Other System Impacts

Secure shell relies on the network infrastructure to operate.

3.5 License Impacts

ECS has licensed support for all UNIX and Linux platforms at each of the four DAACs, the SMC, PVC, VATC, and EDF String 2 and String 3 labs.

3.6 Vendor Known Bugs

The vendor admits to a few fairly trivial bugs, which will not affect ECS operation:

- Backspace does not work in sftp window in a nested connection (no impact)
- Password aging is not functional on Solaris 8 (no impact)

This page intentionally left blank.

4 Inventory

4.1 Tar File Listing

This tar file contains the following files and directories:

Checksum	Blocksize	Filename
		ssh330.tar.gz

Table 5.1-□. Physical Media

None.

This page intentionally left blank.

5 Non-Conformance Status

5.1 NCR(s) Included in Release

The following table lists ECSed37486 and ECSed38486. This list includes NCRs only in the T, V, or C states and are listed in ascending order.

Table 5.1-1. NCRs Included in Release

NCR	Project	Sev	State	Test Site	Description	Comment/ Patch Name
38446	OPS_COTS	3	T	IDG Cell	scp does not allow colons in local filenames	
38486	OPS_COTS	2	T	LaRC	Data Transfers for MISR and TES data to JPL extremely slow	

5.2 Open NCR(s) Against This Release

None.

5.3 NCRs in Custom Code Patches

None.

This page intentionally left blank.

6 Machines Impacted

*__NOTE:__ ssh 3.3.0 should also be installed on all M&O UNIX machines as well.

Site	Host Name	Subsystem	Host Function
EDC	e0asp04 *	AST	ASTER DEM W/S 01
	e0asp05 *	AST	ASTER DEM W/S 02
	e0ass01 *	AST	ASTER LUT DBMS Srvr 01
	e0ass02 *	AST	ASTER LUT DBMS Srvr 02
	e0ins01	CLS	Sun Consolidation External Server
	e0css02	CSS	CSS Srvr
	e0dms03	DMS	Data Spec W/S 01
	e0dms04	DMS	Data Spec W/S 02
	e0ais02	DPS	AIT W/S
	e0ais03	DPS	AIT W/S / DBMS Srvr 01
	e0sps04	DPS	Queuing Srvr
	e0spg11	DPS	Science Processor 01
	e0acg11	DPS	APC Srvr
	e0acs11	DPS	Sun Consolidation Internal Server
	e0acs12	DPS	Operations Workstation
	e0dig06	DSS	PDS Srvr
	e0drs03	DSS	ACSLS W/S 01
	e0drs04	DSS	ACSLS W/S 02
	e0drs08	DSS	ACSLS W/S 03
	e0drg11	DSS	FSMS Srvr 1
	e0drg12	DSS	FSMS Srvr 2
	e0icg11	INS	Ingest Srvr
	e0mss02	MSS	CM Srvr
	e0mss01	MSS	MSS File Srvr
	e0console1	MSS	SGI Console1
	e0mss04	MSS	Tape Backup Srvr
	e0pls03	PLS	Planning/Mgmt W/S 01
	e0dps01	PLS	Data Pool Srvr
	e0sas01	SYN	Metadata Srvr
	e0isp01	ISS	Security W/S
	e0dus01	DUE	Subscription Subsetter
GSFC	g0dms05	CLS	Data Spec W/S 03
	g0css02	CSS	CSS Srvr
	g0dms03	DMS	Data Spec W/S 01

* Installation is recommended for these hosts, but software baseline is managed only by the DAAC.

Site	Host Name	Subsystem	Host Function
	g0dms04	DMS	Data Spec W/S 02
	g0ins01	DMS	Sun Consolidation External Server
	g0ais05	DPS	AIT W/S
	g0ais01	DPS	AIT W/S and DBMS Srvr 01
	g0ais09	DPS	W/S and DBMS Srvr 02
	g0ais10	DPS	W/S and DBMS Srvr 03
	g0mog01	DPS	MODAPS Srvr
	g0spg01	DPS	Science Processor 01
	g0spg10	DPS	Science Processor 02
	g0spg11	DPS	Science Processor 03
	g0acg01	DSS	APC Srvr (P)
	g0acs02	DSS	Operations W/S 01
	g0acs06	DSS	Operations W/S 02
	g0acs11	DSS	Sun Consolidation Internal Server
	g0dig06	DSS	PDS Srvr
	g0drs04	DSS	ACSLS W/S 01
	g0drs03	DSS	ACSLS W/S 02
	g0drs15	DSS	ACSLS W/S 03
	g0drs12	DSS	ACSLS W/S 04
	g0drs05	DSS	ACSLS W/S 05
	g0drg01	DSS	FSMS Server (P1)
	g0drg02	DSS	FSMS Server (P2)
	g0drg04	DSS	FSMS Server (P3)
	g0drg05	DSS	FSMS Server (P5)
	g0icg01	INS	Ingest Srvr (P)
	g0mss02	MSS	CM Srvr
	g0mss10	MSS	MSS File Srvr
	g0console1	MSS	SGI Console1
	g0console2	MSS	SGI Console2
	g0mss07	MSS	Tape Backup Srvr
	g0pls01	PLS	Planning/Management W/S 1
	g0pls03	PLS	Planning/Management W/S 2
	g0dps01	SYN	Data Pool Srvr
	g0sas01	SYN	Metadata Srvr
	g0spp12	DPS	MODIS DB science proc 1
	g0spp14	DPS	MODIS DB science proc 2
	g0isp01	ISS	Security W/S
	g0dus01	DUE	Subscription Subsetter
LaRC	l0dms05	CLS	Data Spec W/S 03
	l0ins01	CLS	Sun consolidation external server
	l0css02	CSS	CSS Server
	l0dms01	DMS	Data Spec W/S 01
	l0dms04	DMS	Data Spec W/S 02

Site	Host Name	Subsystem	Host Function
	l0ais09	DPS	AIT W/S
	l0ais01	DPS	AIT W/S / DBMS Srvr 01
	l0sps03	DPS	Queuing Srvr
	l0spg11	DPS	Science Processor 01
	l0spg10	DPS	Science Processor 02
	l0ais10	DPS	X-Term Srvr
	l0acg02	DPS	APC Srvr
	l0acs03	DSS	Sun Consolidation Internal Server
	l0acs01	DSS	Operations WS 01
	l0acs06	DSS	Operations WS 02
	l0dig06	DSS	PDS Srvr
	l0drs02	DSS	ACSLS W/S 01
	l0drg01	DSS	FSMS Srvr 1
	l0drg03	DSS	FSMS Srvr 2
	l0mss01	MSS	CM Srvr
	l0mss10	MSS	MSS File Srvr
	l0console1	MSS	SGI Console1
	l0console2	MSS	SGI Console1
	l0mss05	MSS	Tape Backup Srvr Planning/Management WS 01
	l0pls02	PLS	
	l0dps01	SYN	Data Pool Srvr
	l0sas01	SYN	Metadata Srvr
	l0isp01	ISS	Security W/S
NSIDC	n0css02	CSS	CSS Srvr
	n0dms04	DMS	Data Spec W/S 01
	n0ins02	DMS	Sun Consolidation External Server
	n0ais01	DPS	AIT W/S / DBMS Srvr 01
	n0spg03	DPS	Science Processor 01
	n0ais05	DPS	Xrunner/loadrunner Srvr
	n0acg01	DSS	APC Srvr
	n0acs03	DSS	Operations WS 01
	n0acs06	DSS	Operations WS 02
	n0acs04	DSS	Sun Consolidation Internal Server
	n0dig06	DSS	PDS Srvr
	n0drs03	DSS	ACSLS W/S 01
	n0drg01	DSS	FSMS Srvr
	n0mss21	DSS	Applications Srvr
	n0mss02	MSS	CM Srvr
	n0mss01	MSS	MSS File Srvr
	n0console1	MSS	SGI Console1
	n0mss05	MSS	Tape Backup Srvr
	n0dps01	DPL	Data Pool Srvr
	n0isp01	ISS	Security W/S

Site	Host Name	Subsystem	Host Function
	n0sas01	DPL	Metadata Srvr
VATC	t1ins02	DMS	Sun Consolidation External Srvr
	t0ins01	DMS	VATC SMC Interface Srvr
	t1css01	CSS	CSS Srvr
	t1dms02	DMS	DataSpec W/S
	t1ais01	DPS	AIT W/S
	t1aqg02	DPS	QA W/S
	t1sps02	DPS	Queuing
	t1spg03	DPS	Science Proc.
	t1acg04	DSS	APC Srvr
	t1acs02	DSS	Ops W/S
	t1acs06	DSS	Sun Consolidation Internal Srvr
	t1dps01	DSS	Distribution Srvr
	t1dpg06	DSS	PDS Srvr
	t1drs02	DSS	ACSLS
	t1drg03	DSS	FSMS Srvr
	t1mss06	MSS	Applications Srvr
	t1mss03	MSS	CM Srvr
	t1code1	MSS	Code Drop Box
	t1mss04	MSS	MSS File Srvr
	t1console1	MSS	SGI console
	t1mss02	MSS	Tape Backup
	t0mss01	MSS	Mgmt Srvr
	t0ins01	MSS	VATC SMC Interface Srvr
	t1pls02	PLS	Planning/Mgmt
	t1mss06	SYN	Metadata Srvr
SMC	m0css03	CLS	Interface Srvr 01
	m0css04	CSS	FTP Srvr 02
	m0css05	M&0	IGS ftp Server 1
	m0mss17	M&O	M+O Knowledge Base Srvr
	m0mss16	MSS	Applications Srvr (P1)
	m0mss15	MSS	Applications Srvr (S1)
	m0mss02	MSS	CM Srvr
	m0mss01	MSS	MSS File Srvr
	m0mss04	MSS	Tape Backup Srvr
	m0isp01	ISS	Security W/S
PVC	p2ass01	AST	ASTER LUT Srvr
	p2ins02	CLS	Sun Consolidation External Server
	p0css02	CSS	CSS Srvr
	p2dms01	DMS	Ops W/S
	p2ins01	CLS	Interface Srvr
	p0ins02	CLS	Interface Srvr
	p0ais01	DPS	DBMS Srvr and W/S

Site	Host Name	Subsystem	Host Function
	p2sps06	DPS	Queuing Srvr
	p0spg01	DPS	Science Proc.
	p0spg07	DPS	Science Proc.
	p0acg05	DSS	APC Srvr
	p2acs06	DSS	Sun Consolidation Internal Server
	p2acs02	DSS	Ops W/S
	p0drs03	DSS	ACSLS
	p0drs05	DSS	ACSLS
	p0drg01	DSS	FSMS Srvr
	p0drg04	DSS	FSMS Srvr
	p0icg01	INS	Ingest
	p0mss02	MSS	Systems Mgmt
	p0mss10	MSS	Automount Srvr
	p0console1	MSS	SGI Console
	p0mss07	MSS	Tape Backup Server
	p2pls02	MSS	PDPS DBMS Server
	p2pls01	PLS	Planning/Management WS 01
	p2dps01	PLS	Data Pool Server
	p0sas01	SYN	Metadata Server
	p0teg01	TST	MODAPS
	p0tes02	TST	EDOS/LPS
	p0tes03	TST	Push area
	p2mss20	MSS	DNS/NIS srvr
	p2mss21	MSS	Dashboard srvr
	p0isp01	ISS	Security W/S

This page intentionally left blank.

7 COTS Installation Instructions

7.1 Prerequisites

There are no prerequisites. Approximate installation time for average systems administrator per host: 15 minutes

Space required: 100MB for install 0-10MB in operations

No reboot is required.

7.2 Uninstall Instructions

None.

7.3 Installation Instructions

7.3.1 Sun installation

1. Login to host as root or su to root.
2. Copy the ssh330.tar.gz file to /tmp or other convienient location. If the release will be installed on multiple machines, it is recommended to install from an automounted directory such as /automnt/net/admin.
3. Change directory to that location. For example:

   # **cd /*stagingdisk*** ↵
4. Explode the file using the command:

   # **gzip –dc ssh330.tar.gz | tar –xovf -** ↵
5. Change directory to the ssh330 install directory using the command:

   # **cd ssh330** ↵
6. Explode the Sun tarfile using the command:

   # **tar -xvf ssh330.sunpkg.tar** ↵
7. Optionally, you may backup the existing files using the command:

   # **cpssh.sh** ↵

   NOTE: By default, this puts all the files in /tmp/bssh and creates a tar file /tmp/<*hostname*>.bssh24.tar
8. Verify that the system has the old versions of ssh using the command:

   # **pkginfo | grep ssh** ↵

system fssh32 F-Secure Secure Shell 3.2.3

If the response is positive, do step 9. Otherwise skip to step 10.

9. Remove the old package. Using the results from step 8 for example, use the command:

   # **pkgrm fssh32** ↵

   (answer "**y**" to any questions asked)

   ...

10. If not already present on the system, you should install the TCP Wrappers package using the command:

    # **pkgadd –d /*stagingdisk*/ssh330 tcpw76** ↵

    (answer "**y**" to any questions asked)

    ...

11. Install the new ssh package:

    # **pkgadd –d / *stagingdisk* /ssh330 fssh330** ↵

    (answer "**y**" to any questions asked)

    ...

12. *If this is a new installation*, edit /etc/ssh2/ssh2_config to uncomment the appropriate lines for

    SocksServer (not needed for EDF)

    DefaultDomain

    NOTE: If this package updates an existing installation, no changes to the configuration files are required

13. Remove the install directory.

    # **rm –rf /*stagingdisk* /ssh330** ↵

14. If desired, you may turn on log rotation using the commands:

    # /usr/local/sbin/ssh.log_rot ↵

    # /usr/local/sbin/wrap.log_rot ↵

    NOTE: If log rotation has been previously setup, you need not do this step.

15. Logoff from root and login as a normal user.

16. Do some quick checks to verify that the install worked, such as:

    % **ps –ef | grep sshd2** ↵ (should show at least one process spawned recently by PID 1)

    % **ssh2 <*differenthost*>** ↵

% **scp2** ***localtestfile remotehost*****:** ↵

17. Logoff.

7.3.2 SGI Installation

1. Login to host as root or su to root.
2. Copy the ssh330.tar.gz file to /tmp or other convienient location . If the release will be installed on multiple machines, it is recommended to install from an automounted directory such as /automnt/net/admin.
3. Change directory to that location. For example:

   # **cd /*stagingdisk*** ↵
4. Explode the file using the command:

   # **gzip –dc ssh330.tar.gz | tar –xovf -** ↵
5. Change directory to the ssh32 install directory using the command:

   # **cd ssh330** ↵
6. Explode the SGI tarfile using the command:

   # **tar -xvf ssh330+.sgiinst.tar** ↵
7. Optionally, you may backup the existing files using the command:

   # **cpssh.sh** ↵

   NOTE: By default, this puts all the files in /tmp/bssh and creates a tar file /tmp/<hostname>.bssh24.tar
8. Verify that the system has the old versions of ssh using the command:

   # **versions | grep ssh** ↵

```
I  fssh32               09/09/2003  F-Secure SSH 3.2.3
I  fssh32.books         09/09/2003  Books
I  fssh32.books.userguide  09/09/2003  User Guide
I  fssh32.man           09/09/2003  Man Pages
I  fssh32.man.manpages  09/09/2003  Man Pages
I  fssh32.man.relnotes  09/09/2003  Release Notes
I  fssh32.sw            09/09/2003  ssh applications
I  fssh32.sw.base       09/09/2003  Base Software
```

If the response is positive, do step 9. Otherwise skip to step 10.

9. Remove the old packages. Using the results of step 8 for example, use the command:

   # **versions remove fssh32** ↵

   NOTE: If either package fails to be removed, note the error. If it is a file missing, copy the file from the backup you made in /tmp/bssh.

10. Change directory to the sgi install directory

    # **cd sgi** ↵

    NOTE: this should put you in /tmp/ssh330/sgi

11. Install the new package:

    # **inst** ↵

    inst> **from** ↵

    inst> **.** ↵

    inst> **step** ↵

    (make sure there are "i"s next to each of the fssh330 modules. If this is a new install also install the tcpw76 modules)

    inst> **go** ↵

    (answer yes to any questions asked. There should be *no* conflicts...)

    inst> **quit** ↵

12. *If this is a new install*, edit /etc/ssh2/ssh2_config to uncomment the appropriate lines for

    SocksServer (not needed for EDF)

    DefaultDomain

15. Remove the install directory as required.

    # **rm –rf /** ***stagingdisk*** **/ssh330** ↵

16. If desired, you may turn on log rotation using the commands:

    # /usr/local/sbin/ssh.log_rot ↵

    # /usr/local/sbin/wrap.log_rot ↵

    NOTE: If log rotation has been previously setup, you need not do this step.

17. Logoff as root and login as a normal user.

18. Do some quick checks to verify that the install worked, such as:

    % **ps –ef | grep sshd2** ↵ (should show at least one process spawned recently by PID 1)

% **ssh2 <*differenthost*>** ↵

% **scp2 *localtestfile remotehost*:** ↵

19. Logoff

7.3.2 Linux installation

1. Login to host as root or su to root.
2. Copy the ssh330.tar.gz file to /tmp or other convienient location. If the release will be installed on multiple machines, it is recommended to install from an automounted directory such as /automnt/net/admin.
3. Change directory to that location. For example:

   # **cd /*stagingdisk*** ↵
4. Explode the file using the command:

   # **gzip –dc ssh330.tar.gz | tar –xovf -** ↵
5. Change directory to the ssh330 install directory using the command:

   # **cd ssh330** ↵
6. Verify that the system has the old versions of ssh using the command:

   # **rpm -qa | grep ssh** ↵

   fssh32 F-Secure Secure Shell 3.2.3
7. If the response is positive, do step 9. Otherwise skip to step 10.
8. Remove the old package. Using the results from step 8 for example, use the command:

   # **rpm -e fssh32** ↵
9. If not already present on the system, you should install the TCP Wrappers package from the CDs that came with the OS using the command:

   # **rpm –Uvh wrappers.rpm** ↵
10. Install the new ssh package:

    # **rpm -Uvh fssh-3.3.0-14ecs.i386.rpm** ↵
11. *If this is a new installation*, edit /etc/ssh2/ssh2_config to uncomment the appropriate lines for

    SocksServer (not needed for EDF)

    DefaultDomain

NOTE: If this package updates an existing installation, no changes to the configuration files are required

12. *If this is a new installation*, it is recommended that you install the TCP Wrappers RPM from the Red Hat 7.3 install disk 1. Determine if the rpm is present using the command:

    # **rpm –qa | grep tcp_wrap** ↵

13. If there is no response to the rpm query, insert the cd in the cdrom drive and use the command:

    # **rpm –Uvh /mnt/cdrom/RedHat/rpms/tcp_wrappers-7.6-19.i386.rpm**↵

14. Remove the install directory as required.

    # **rm –rf /*stagingdisk* /ssh330** ↵

15. If desired, you may turn on log rotation using the commands:

    # /usr/local/sbin/ssh.log_rot ↵

    # /usr/local/sbin/wrap.log_rot ↵

    NOTE: If log rotation has been previously setup, you need not do this step.

16. Logoff from root and login as a normal user.

17. Do some quick checks to verify that the install worked, such as:

    % **ps –ef | grep sshd2** ↵ (should show at least one process spawned recently by PID 1)

    % **ssh2 <*differenthost*>** ↵

    % **scp2 *localtestfile remotehost*:** ↵

18. Logoff.

7.4 Custom Code Integration

None.

7.5 Interrogation Checkout

On an SGI, the "ssh2 –V" command should reveal:

ssh2: F-Secure SSH 3.3.0 (build 14) on mips-sgi-irix6.5

On a Sun, the "ssh2 –V" command should reveal:

ssh2: F-Secure SSH 3.3.0 (build 14) on sparc-sun-solaris2.8

NOTE: Any ssh command will reveal its' version using the "-V" flag.

7.6 Back-Out Instructions

On a Sun system:

pkgrm fssh330 ↵

and then reinstall ECS SSH 3.2.3 as identified in CM document 914-TDA-259 (ECS Secure Shell 3.2.3 for the ECS Project)

On an SGI system:

versions remove fssh330 ↵

and then reinstall ECS SSH 3.2.3 as identified in CM document 914-TDA-259 (ECS Secure Shell 3.2.3 for the ECS Project)

On a Linux system:

rpm –e fssh-3.3.0-14ecs ↵

and then reinstall using these same instructions with the fssh-3.2.3-9ecs.i386.rpm file.

This page intentionally left blank.

APPENDIX A Test Verification

A.1 Test Procedures

	SSH 3.2 Testing Version 0.1	Old IRIX:	P0spg01				
	Legend: OFC= F-secure 2.4 Client	Old Solaris:	P0tes02				
	NFC= F-secure 3.2 Client	New IRIX:	P0acg05				
	OFS=F-secure 2.4 Server	New Solaris:	Ptsps12				
	NFS=F-secure 3.2 Server	Fsecure linux:	Ptspp11				
	OC=Openssh 3.5 Client	Openssh linux:	Pt0spp01				
	OS=Openssh 3.5 Server						
	Note: File size for transfers = 100MB	assumes sha1					
TC	Requirements:	Host A	Host B	P/F			
	1. The new ssh2 client MUST work with the old server:				Ps -ef		
	A. NFC-OFS/3des/password				Top		
1	IRIX to Solaris	OK	OK		~s		
2	Solaris to IRIX	OK	OK		Xterm	Xterm	
3	linux to Solaris	OK	OK		Wish	Wish	
4	linux to IRIX	OK	OK		N0acg01/ n0drg01	N0ins02 /n0ins0 1	OFS
	B. NFC-OFS/3des/passphrase				Fugue	Toccata	NFC
5	IRIX to Solaris	OK	OK	P			
6	Solaris to IRIX	OK	OK	P			
7	linux to Solaris	OK	OK	P			
8	linux to IRIX	OK	OK	P			
	C. NFC-OFS/3des/hostbased						
9	IRIX to Solaris	NT	NT	P			
10	Solaris to IRIX	NT	NT	P			
11	linux to Solaris	NT	NT	P			

12	linux to IRIX	NT	NT	P			
	D. NFC-OFS/3des/agent						
13	IRIX to Solaris	OK	OK	P			
14	Solaris to IRIX	OK	OK	P			
15	linux to Solaris	OK	OK	P			
16	linux to IRIX	OK	OK	P			
	E. NFC-OFS/3des/hostbased remote command or script						
17	IRIX to Solaris	OK		P			
18	Solaris to IRIX	OK		P			
19	linux to Solaris	OK		P			
20	linux to IRIX	OK		P			
	2. The old ssh2 client MUST work with the new server:						
	A. OFC - NFS/3des/password						
21	IRIX to Solaris	OK	OK	P			
22	IRIX to linux	OK	OK	P			
23	Solaris to IRIX	OK	OK	P			
24	Solaris to linux	OK	OK	P			
	B. OFC - NFS/3des/passphrase						
25	IRIX to Solaris	NT	NT	-			
26	IRIX to linux	NT	NT	-			
27	Solaris to IRIX	NT	NT	-			
28	Solaris to linux	NT	NT	-			
	C. OFC-NFS/3des/hostbased						
29	IRIX to Solaris	NT	NT	-			
30	IRIX to linux	NT	NT	-			
31	Solaris to IRIX	NT	NT	-			
32	Solaris to linux	NT	NT	-			
	D. OFC-NFS/3des/agent						
33	IRIX to Solaris	OK	OK	P			
34	IRIX to linux	OK	OK	P			
35	Solaris to IRIX	OK	OK	P			
36	Solaris to linux	OK	OK	P			
	E. OFC-NFS/3des/hostbased remote command or script						
37	IRIX to Solaris	OK	OK	P			
38	IRIX to linux	OK	OK	P			

39	Solaris to IRIX	OK	OK	P			
40	Solaris to linux	OK	OK	P			
	3. The new ssh2 client MUST work with the new server:						
	A. NFC - NFS /aes128/password						
41	IRIX to Solaris	OK	OK	P			
42	IRIX to linux	OK	OK	P			
43	Solaris to IRIX	OK	OK	P			
44	Solaris to linux	OK	OK	P			
45	linux to Solaris	OK	OK	P			
46	linux to IRIX	OK	OK	P			
	B. NFC - NFS /aes128/passphrase						
47	IRIX to Solaris	NT	NT	-			
48	IRIX to linux	NT	NT	-			
49	Solaris to IRIX	NT	NT	-			
50	Solaris to linux	NT	NT	-			
51	linux to Solaris	NT	NT	-			
52	linux to IRIX	NT	NT	-			
	C. NFC - NFS /aes128/hostbased						
53	IRIX to Solaris	OK	OK	P	G0acg01 – g0acs06 – g0acs04		
54	IRIX to linux	OK	OK(old srvr)	P			
55	Solaris to IRIX	OK	OK	P			
56	Solaris to linux	OK	OK(old srvr)	P			
57	linux to Solaris	OK	OK	P			
58	linux to IRIX	OK	OK(old srvr)	P			
	D. NFC - NFS /aes128/agent						
59	IRIX to Solaris	OK	OK	P			
60	IRIX to linux	OK	OK	P			
61	Solaris to IRIX	OK	OK	P			
62	Solaris to linux	OK	OK	P			
63	linux to Solaris	OK	OK	P			
64	linux to IRIX	OK	OK	P			
	E. NFC - NFS /aes128/hostbased remote command or script				Top		
65	IRIX to Solaris	OK		P			
66	IRIX to linux	OK		P			
67	Solaris to IRIX	OK		P			
68	Solaris to linux	OK		P			

69	linux to Solaris	OK		P			
70	linux to IRIX	OK		P			
	F. NFC - NFS /3des/password						
71	IRIX to Solaris	OK	OK	P			
72	IRIX to linux	OK	OK	P			
73	Solaris to IRIX	OK	OK	P			
74	Solaris to linux	OK	OK	P			
75	linux to Solaris	OK	OK	P			
76	linux to IRIX	OK	OK	P			
	G. NFC - NFS /3des/passphrase						
77	IRIX to Solaris	NT	NT	-			
78	IRIX to linux	NT	NT	-			
79	Solaris to IRIX	NT	NT	-			
80	Solaris to linux	NT	NT	-			
81	linux to Solaris	NT	NT	-			
82	linux to IRIX	NT	NT	-			
	H. NFC - NFS /3des/hostbased						
83	IRIX to Solaris	NT	NT	-			
84	IRIX to linux	NT	NT	-			
85	Solaris to IRIX	NT	NT	-			
86	Solaris to linux	NT	NT	-			
87	linux to Solaris	NT	NT	-			
88	linux to IRIX	NT	NT	-			
	I. NFC - NFS /3des/agent						
89	IRIX to Solaris	NT	NT	-			
90	IRIX to linux	NT	NT	-			
91	Solaris to IRIX	NT	NT	-			
92	Solaris to linux	NT	NT	-			
93	linux to Solaris	NT	NT	-			
94	linux to IRIX	NT	NT	-			
	J. NFC - NFS /3des/hostbased remote command or script						
95	IRIX to Solaris	NT	NT	-			
96	IRIX to linux	NT	NT	-			
97	Solaris to IRIX	NT	NT	-			
98	Solaris to linux	NT	NT	-			
99	linux to Solaris	NT	NT	-			
100	linux to IRIX	NT	NT	-			

	4. The new ssh2 client SHOULD work with an Openssh server:						
	A. NFC - OS /aes128/password						
101	IRIX to linux	OK	OK	P			
102	Solaris to linux	OK	OK	P			
103	linux to linux	OK	OK	P			
	B. NFC - OS /aes128/passphrase						
104	IRIX to linux	OK	OK	P			
105	Solaris to linux	OK	OK	P			
106	linux to linux	OK	OK	P			
	C. NFC - OS /aes128/hostbased						
107	IRIX to linux	NT	NT	-			
108	Solaris to linux	NT	NT	-			
109	linux to linux	NT	NT	-			
	D. NFC - OS /aes128/agent						
110	IRIX to linux	NT	NT	-			
111	Solaris to linux	NT	NT	-			
112	linux to linux	NT	NT	-			
	E. NFC - OS /aes128/hostbased remote command or script						
113	IRIX to linux	NT	NT	-			
114	Solaris to linux	NT	NT	-			
115	linux to linux	NT	NT	-			
		NT	NT	-			
	5. An Openssh client SHOULD work with a new server:						
	A. OC - NFS /aes128/password						
116	linux to IRIX	Fail	Fail	F			
117	linux to Solaris	Fail	Fail	F			
118	linux to linux	Fail	Fail	F			
	B. OC - NFS /aes128/passphrase						
119	linux to IRIX	Fail	Fail	F			
120	linux to Solaris	Fail	Fail	F			
121	linux to linux	Fail	Fail	F			
	C. OC - NFS /aes128/hostbased						
122	linux to IRIX	Fail	Fail	F			

123	linux to Solaris	Fail	Fail	F			
124	linux to linux	Fail	Fail	F			
	D. OC - NFS /aes128/agent						
125	linux to IRIX	Fail	Fail	F			
126	linux to Solaris	Fail	Fail	F			
127	linux to linux	Fail	Fail	F			
	E. OC - NFS /aes128/hostbased remote command or script						
128	linux to IRIX	Fail	Fail	F			
129	linux to Solaris	Fail	Fail	F			
130	linux to linux	Fail	Fail	F			
	6. The new scp2 client MUST work with the old server:				Ssa works when the middle host does not have keys – it is the originating host!		
	A. NFC-OFS/3des/password						
131	IRIX to Solaris	OK		P	Scp will not work without environment file		
132	Solaris to IRIX	OK		P			
133	linux to Solaris	OK		P	Scp2 target		
134	linux to IRIX	OK		P	Ls		
	B. NFC-OFS/3des/passphrase				Cd /tmp		
135	IRIX to Solaris	OK		P	Put t		
136	Solaris to IRIX	OK		P	Lrm t ; get t		
137	linux to Solaris	OK		P	Ssh2 target cksum t		
138	linux to IRIX	OK		P	Cksum t		
	C. NFC-OFS/3des/hostbased				Cksum t		
139	IRIX to Solaris	NT		-			
140	Solaris to IRIX	NT		-			
141	linux to Solaris	NT		-			
142	linux to IRIX	NT		-			
	D. NFC-OFS/3des/agent						
143	IRIX to Solaris	OK		P			
144	Solaris to IRIX	OK		P			
145	linux to Solaris	OK		P			
146	linux to IRIX	OK		P			
	7. The old scp2 client MUST work with the new server:						
	A. OFC - NFS/3des/password						
147	IRIX to Solaris	OK		P			

148	IRIX to linux	OK		P			
149	Solaris to IRIX	OK		P			
150	Solaris to linux	OK		P			
	B. OFC - NFS/3des/passphrase						
151	IRIX to Solaris	NT		-			
152	IRIX to linux	NT		-			
153	Solaris to IRIX	NT		-			
154	Solaris to linux	NT		-			
	C. OFC-NFS/3des/agent						
155	IRIX to Solaris	OK		P			
156	IRIX to linux	OK		P			
157	Solaris to IRIX	OK		P			
158	Solaris to linux	OK		P			
	D. OFC - NFS/none/passphrase						
159	IRIX to Solaris	NT		-			
160	IRIX to linux	NT		-			
161	Solaris to IRIX	NT		-			
162	Solaris to linux	NT		-			
	E. OFC - NFS/none/agent						
163	IRIX to Solaris	OK		P			
164	IRIX to linux	OK		P			
165	Solaris to IRIX	OK		P			
166	Solaris to linux	OK		P			
	8. The new scp2 client MUST work with the new server:						
	A. NFC - NFS /aes128/password						
167	IRIX to Solaris	NT		-			
168	IRIX to linux	NT		-			
169	Solaris to IRIX	NT		-			
170	Solaris to linux	NT		-			
171	linux to Solaris	NT		-			
172	linux to IRIX	NT		-			
	B. NFC - NFS /aes128/passphrase						
173	IRIX to Solaris	NT		-			
174	IRIX to linux	NT		-			
175	Solaris to IRIX	NT		-			
176	Solaris to linux	NT		-			
177	linux to Solaris	NT		-			

178	linux to IRIX	NT		-			
	C. NFC - NFS /aes128/hostbased						
179	IRIX to Solaris	NT		-			
180	IRIX to linux	NT		-			
181	Solaris to IRIX	NT		-			
182	Solaris to linux	NT		-			
183	linux to Solaris	NT		-			
184	linux to IRIX	NT		-			
	D. NFC - NFS /aes128/agent						
185	IRIX to Solaris	OK		P			
186	IRIX to linux	OK		P			
187	Solaris to IRIX	OK		P			
188	Solaris to linux	OK		P			
189	linux to Solaris	OK		P			
190	linux to IRIX	OK		P			
	E. NFC - NFS /3des/password						
191	IRIX to Solaris	NT		-			
192	IRIX to linux	NT		-			
193	Solaris to IRIX	NT		-			
194	Solaris to linux	NT		-			
195	linux to Solaris	NT		-			
196	linux to IRIX	NT		-			
	F. NFC - NFS /3des/passphrase						
197	IRIX to Solaris	NT		-			
198	IRIX to linux	NT		-			
199	Solaris to IRIX	NT		-			
200	Solaris to linux	NT		-			
201	linux to Solaris	NT		-			
202	linux to IRIX	NT		-			
	G. NFC - NFS /3des/hostbased						
203	IRIX to Solaris	NT		-			
204	IRIX to linux	NT		-			
205	Solaris to IRIX	NT		-			
206	Solaris to linux	NT		-			
207	linux to Solaris	NT		-			
208	linux to IRIX	NT		-			
	H. NFC - NFS /3des/agent						
209	IRIX to Solaris	OK		P			
210	IRIX to linux	OK		P			
211	Solaris to IRIX	OK		P			

212	Solaris to linux	OK		P			
213	linux to Solaris	OK		P			
214	linux to IRIX	OK		P			
	I. NFC - NFS /none/passphrase						
215	IRIX to Solaris	NT		-			
216	IRIX to linux	NT		-			
217	Solaris to IRIX	NT		-			
218	Solaris to linux	NT		-			
219	linux to Solaris	NT		-			
220	linux to IRIX	NT		-			
	J. NFC - NFS /none/agent						
221	IRIX to Solaris	OK		P			
222	IRIX to linux	OK		P			
223	Solaris to IRIX	OK		P			
224	Solaris to linux	OK		P			
225	linux to Solaris	OK		P			
226	linux to IRIX	OK		P			
	9. An Openssh scp client SHOULD work with a new server:						
	A. OC - NFS /aes128/password						
228	linux to IRIX	Fail		F			
229	linux to Solaris	Fail		F			
230	linux to linux	Fail		F			
	B. OC - NFS /aes128/passphrase						
231	linux to IRIX	Fail		F			
232	linux to Solaris	Fail		F			
233	linux to linux	Fail		F			
	C. OC - NFS /aes128/hostbased						
234	linux to IRIX	Fail		F			
235	linux to Solaris	Fail		F			
236	linux to linux	Fail		F			
	D. OC - NFS /aes128/agent						
237	linux to IRIX	Fail		F			
238	linux to Solaris	Fail		F			
239	linux to linux	Fail		F			
	E. OC - NFS /none/passphrase						
240	linux to IRIX	Fail		F			

241	linux to Solaris	Fail		F			
242	linux to linux	Fail		F			
	F. OC - NFS /none/agent						
242	linux to IRIX	Fail		F			
243	linux to Solaris	Fail		F			
244	linux to linux	Fail		F			
	10. An new scp2 client SHOULD work with an OpenSSH server:						
	A. NFC - OS /aes128/password						
228	IRIX to linux	OK		P			
229	Solaris to linux	OK		P			
230	linux to linux	OK		P			
	B. NFC - OS /aes128/passphrase						
231	IRIX to linux	NT		-			
232	Solaris to linux	NT		-			
233	linux to linux	NT		-			
	C. NFC - OS /aes128/hostbased						
234	IRIX to linux	NT		-			
235	Solaris to linux	NT		-			
236	linux to linux	NT		-			
	D. NFC - OS /aes128/agent						
237	IRIX to linux	OK		P			
238	Solaris to linux	OK		P			
239	linux to linux	OK		P			
	E. NFC - OS /none/passphrase						
240	linux to IRIX	Fail		F			
241	linux to Solaris	Fail		F			
230	linux to linux	Fail		F			
	F. NFC - OS /none/agent						
242	IRIX to linux	Fail		F			
243	Solaris to linux	Fail		F			
244	linux to linux	Fail		F			
	11. The new sftp2 client MUST work with the old server:						
	A. NFC-OFS/3des/password						
245	IRIX to Solaris	OK		P	Sftp2 target		
246	Solaris to IRIX	OK		P	Ls		

247	linux to Solaris	OK		P	Cd /tmp		
248	linux to IRIX	OK		P	Put t		
	B. NFC-OFS/3des/passphrase				Lrm t ; get t ; quit		
249	IRIX to Solaris	NT		-	Ssh2 target cksum t		
250	Solaris to IRIX	NT		-	Cksum t		
251	linux to Solaris	NT		-	Cksum t		
252	linux to IRIX	NT		-			
253	C. NFC-OFS/3des/hostbased						
	IRIX to Solaris	NT		-			
254	Solaris to IRIX	NT		-			
255	linux to Solaris	NT		-			
256	linux to IRIX	NT		-			
	D. NFC-OFS/3des/agent						
257	IRIX to Solaris	OK		P			
258	Solaris to IRIX	OK		P			
259	linux to Solaris	OK		P			
260	linux to IRIX	OK		P			
	12. The old sftp2 client MUST work with the new server:						
	A. OFC - NFS/3des/password						
261	IRIX to Solaris	OK		P			
262	IRIX to linux	OK		P			
263	Solaris to IRIX	OK		P			
264	Solaris to linux	OK		P			
	B. OFC - NFS/3des/passphrase						
265	IRIX to Solaris	NT		-			
266	IRIX to linux	NT		-			
267	Solaris to IRIX	NT		-			
268	Solaris to linux	NT		-			
	C. OFC-NFS/3des/hostbased						
269	IRIX to Solaris	NT		-			
270	IRIX to linux	NT		-			
271	Solaris to IRIX	NT		-			
272	Solaris to linux	NT		-			
	D. OFC - NFS/none/passphrase						

273	IRIX to Solaris	NT		-			
274	IRIX to linux	NT		-			
275	Solaris to IRIX	NT		-			
276	Solaris to linux	NT		-			
	E. OFC - NFS/none/agent						
277	IRIX to Solaris	OK		P			
278	IRIX to linux	OK		P			
279	Solaris to IRIX	OK		P			
280	Solaris to linux	OK		P			
	13. The new sftp2 client MUST work with the new server:						
	A. NFC - NFS /aes128/password						
281	IRIX to Solaris	OK		P			
282	IRIX to linux	OK		P			
283	Solaris to IRIX	OK		P			
284	Solaris to linux	OK		P			
285	linux to Solaris	OK		P			
286	linux to IRIX	OK		P			
	B. NFC - NFS /aes128/passphrase						
287	IRIX to Solaris	NT		-			
288	IRIX to linux	NT		-			
289	Solaris to IRIX	NT		-			
290	Solaris to linux	NT		-			
291	linux to Solaris	NT		-			
292	linux to IRIX	NT		-			
	C. NFC - NFS /aes128/hostbased						
293	IRIX to Solaris	OK		P			
294	IRIX to linux	OK		P			
295	Solaris to IRIX	OK		P			
296	Solaris to linux	OK		P			
297	linux to Solaris	OK		P			
298	linux to IRIX	OK		P			
	D. NFC - NFS /aes128/agent						
299	IRIX to Solaris	OK		P			
300	IRIX to linux	OK		P			
301	Solaris to IRIX	OK		P			
302	Solaris to linux	OK		P			
303	linux to Solaris	OK		P			
304	linux to IRIX	OK		P			

	E. NFC - NFS /3des/password						
305	IRIX to Solaris	OK		P			
306	IRIX to linux	OK		P			
307	Solaris to IRIX	OK		P			
308	Solaris to linux	OK		P			
309	linux to Solaris	OK		P			
310	linux to IRIX	OK		P			
	F. NFC - NFS /3des/passphrase						
311	IRIX to Solaris	NT		-			
312	IRIX to linux	NT		-			
313	Solaris to IRIX	NT		-			
314	Solaris to linux	NT		-			
315	linux to Solaris	NT		-			
316	linux to IRIX	NT		-			
	G. NFC - NFS /3des/hostbased						
317	IRIX to Solaris	NT		-			
318	IRIX to linux	NT		-			
319	Solaris to IRIX	NT		-			
320	Solaris to linux	NT		-			
321	linux to Solaris	NT		-			
322	linux to IRIX	NT		-			
	H. NFC - NFS /3des/agent						
323	IRIX to Solaris	OK		P			
324	IRIX to linux	OK		P			
325	Solaris to IRIX	OK		P			
326	Solaris to linux	OK		P			
327	linux to Solaris	OK		P			
328	linux to IRIX	OK		P			
	I. NFC - NFS /none/passphrase						
329	IRIX to Solaris	NT		-			
330	IRIX to linux	NT		-			
341	Solaris to IRIX	NT		-			
342	Solaris to linux	NT		-			
343	linux to Solaris	NT		-			
344	linux to IRIX	NT		-			
	J. NFC - NFS /none/agent						
345	IRIX to Solaris	OK		P			
346	IRIX to linux	OK		P			
347	Solaris to IRIX	OK		P			
348	Solaris to linux	OK		P			

349	linux to Solaris	OK		P			
350	linux to IRIX	OK		P			
	14. An Openssh sftp client SHOULD work with a new server:						
	A. OC - NFS /aes128/password						
351	linux to IRIX	OK		P			
352	linux to Solaris	OK		P			
353	linux to linux	OK		P			
	B. OC - NFS /aes128/passphrase						
354	linux to IRIX	NT		-			
355	linux to Solaris	NT		-			
356	linux to linux	NT		-			
	C. OC - NFS /aes128/hostbased						
357	linux to IRIX	NT		-			
358	linux to Solaris	NT		-			
359	linux to linux	NT		-			
	D. OC - NFS /aes128/agent						
360	linux to IRIX	OK		P			
361	linux to Solaris	OK		P			
362	linux to linux	OK		P			
	E. OC - NFS /none/passphrase						
363	linux to IRIX	Fail		F			
364	linux to Solaris	Fail		F			
365	linux to linux	Fail		F			
	F. OC - NFS /none/agent						
366	linux to IRIX	Fail		F			
367	linux to Solaris	Fail		F			
368	linux to linux	Fail		F			
	15. An new sftp2 client SHOULD work with an OpenSSH server:						
	A. NFC - OS /aes128/password						
369	IRIX to linux	OK		P			
370	Solaris to linux	OK		P			
371	linux to linux	OK		P			
	B. NFC - OS /aes128/passphrase						

372	IRIX to linux	NT		-			
373	Solaris to linux	NT		-			
374	linux to linux	NT		-			
	C. NFC - OS /aes128/hostbased						
375	IRIX to linux	NT		-			
376	Solaris to linux	NT		-			
377	linux to linux	NT		-			
	D. NFC - OS /aes128/agent						
378	IRIX to linux	OK		P			
379	Solaris to linux	OK		P			
380	linux to linux	OK		P			
	E. NFC - OS /none/passphrase						
381	linux to IRIX	Fail		F			
382	linux to Solaris	Fail		F			
383	linux to linux	Fail		F			
	F. NFC - OS /none/agent						
384	IRIX to linux	Fail		F			
385	Solaris to linux	Fail		F			
386	linux to linux	Fail		F			

A.2 NCRs

None.

A.3 Test Results

Secure Shell 3.3.0 was successfully tested in the VATC, PVC and GES DAAC with no impacts to operational functions.

A.4 EDF Evaluation Plan/Report

EDF Evaluation Plan/Report

Technology Area:	COTS	Date:	9/29/2003
Requester:	Byron Peters	Report No.:	CCR 03-

Proposed Evaluation Group: PVC and EDC

Applicability to ECS: None

Baseline Upgrade

Reason Needed (Issue, need or risk):
Updated Security Features & Vendor Support for version

SE

Office: Office Manager: _____
Signature Date

1. Product Description:
SSH (Secure Shell Commercial) 3.2.3

1.1 Hardware/Platform Requirements: (consider operating system revision level)
Sun/SGI

1.2 Media Requirements:

2. Vendor: (company name, address, etc.)
F-Secure

2.1 Company Background:

2.2 Point of Contact:	Byron Peters	**2.3** Phone Number:	301-925-4077
2.4 Fax Number:		**2.5** Email Address:	Bpeters@eos.hitc.com

3. Evaluation Plan
Install and test ssh 3.2.2. Monitor performance/impact to custom code

3.1 Date Needed:
ASAP

3.2 Length of Evaluation: (please check one)
15 Days ☐ 45 Days ☐ 60 Days ☐ 90 Days ☒ Other ☐

3.3 Product Price: N/A product has been procured and is under maintenance.

3.4 EDF hardware, software and network requirements:
Sun/SGI hosts

3.5 Schedule:

3.6 Projected number of hours to be charged by each evaluator: 10 maximum of 160 man-hours

3.7 Evaluation Criteria: Volume creation

4. Assessment of Product

4.1 Evaluation Against Criteria:

5 Summary of Results

Review Committee Comments:

Priority:

Disposition: